CLAIMS

1. A method for the cipher controlled exploitation of data resources stored in a database associated to a computer system, including the steps of:

- providing a subscriber identity module (SIM) carrying at least one security algorithm;
- producing a cipher key (K) via said at least one security algorithm; and
- using said cipher key (K) for protecting said data resources.

2. The method according to claim 1, characterised in that said step of using said cipher key for protecting said data resources includes the steps of:

- encrypting said data resources by means of said cipher key (K);
- storing said encrypted data resources in said database associated to said computer system;
- retrieving said encrypted data resources from said database; and
- decrypting said encrypted data resources by means of said cipher key (K).

3. The method according to any of claims 1 or 2, characterised in that said step of producing a cipher key includes the steps of:

- generating at least one random value (RAND1, RAND2); and
- subjecting said at least one random value (RAND1, RAND2) to said at least one security algorithm to generate at least one session key (Kc1, Kc2); and
- processing said at least one session key (Kc1, Kc2) via a mixer function (h) to produce said at least one cipher key (K).

4. The method according to claims 3, characterised in that it includes the steps of:

- generating at least two random values (RAND1, RAND2);

- subjecting said at least two random values (RAND1, RAND2) to said at least one security algorithm to generate at least two session keys (Kc1, Kc2); and

- combining said at least two session keys (Kc1, Kc2) via a mixer function (h) to produce said at least one cipher key (K).

5. The method according to any of claims 3 or 4, characterised in that said mixer function includes a hash function (h).

6. The method according to any of claims 3-5, characterised in that it includes the step of inserting in said mixer function (h) a user specific secret (K_u) unrelated to said subscriber identity module security algorithm, whereby said cipher key (K) is unpredictable even based on knowledge of said security algorithm carried in said subscriber identity module (SIM).

7. The method according to any of claims 1-6, characterised in that it includes the step of selecting said data resources from user sensitive data or user credentials.

8. The method according to claim 7, characterised in that said step of using said cipher key (K) for protecting said data resources includes the step of encrypting by means of said cipher key (K) said user sensitive data or said user credentials from plaintext into an encrypted format.

9. The method according to any of claims 7 or 8, characterised in that said step of using said cipher key (K) for protecting said data resources includes the step of decrypting by means of said cipher key (K)

said user sensitive data or said user credentials from an encrypted format into plaintext.

10. The method according to any of claims 8 or 9, characterised in that said user sensitive data or said user credentials in encrypted format have associated a cryptographic header (CH).

11. The method according to claim 10, characterised in that said cryptographic header (CH) comprises an identifier of said subscriber identity module (SIM) and a cryptographic checksum (MAC_K) based on said cipher key (K), said cryptographic checksum (MAC_K) being used for detecting any unauthorized modifications of said encrypted format.

12. The method according to any of claims 7-11, characterised in that said data resources are user credentials said database associated to said computer system is a remote database and said data resources based on said user credentials are stored in said remote database in said encrypted format.

13. The method according to claim 12, characterised in that it includes the step of establishing a relationship between said user credentials stored in said encrypted format in said remote database and a corresponding user subscriber identity module (SIM).

14. The method according to claim 13, characterised in that said relationship is established by means of an identifier of said subscriber identity module (SIM).

15. The method according to claim 14, characterised in that it includes the step of using said identifier for searching within said remote database to permit said user exploitation of said user credentials.

16. A system for the cipher-controlled exploitation of data resources, including:

- at least a subscriber identity module (SIM) carrying at least one security algorithm;
- at least a computer system comprising at least one processing module (CS), said processing module being interfaced with said subscriber identity module (SIM) to generate at least one cipher key (K) via said at least one security algorithm and is configured to protect via said cipher key (K) said data resources; and
- a database associated to said computer system for storing said data resources protected by said cipher key (K).

17. The system according to claim 16, characterised in that said at least one processing module is configured for:

- encrypting said data resources by means of said cipher key (K);
- storing said encrypted data resources in said database associated to said computer system;
- retrieving said encrypted data resources from said database; and
- decrypting said encrypted data resources by means of said cipher key (K).

18. The system according to any of claims 16 or 17, characterised in that said database is included in said computer system.

19. The system according to any of claims 16 or 17, characterised in that said database is remote from said computer system.

20. The system according to any of claims 16-19, characterised in that said processing module is interfaced with said subscriber identity module (SIM) via a smart card reader or a Bluetooth mobile terminal

or an IrDA mobile terminal or a mobile terminal through a cable.

21. The system according to any of claims 16-20, characterised in that said computer system includes a personal computer or a notebook or a laptop or a PDA, or a smart phone.

22. A communication network including a system according to any of claims 16 to 21.

23. A computer program product loadable in the memory of at least one computer and comprising software code portions for performing the method of any of claims 1 to 15.